

Approximate Relational Hoare Logic for Continuous Random Samplings

Tetsuya Sato¹

Research Institute for Mathematical Sciences, Kyoto University, Kyoto, 606-8502, Japan

Abstract

Approximate relational Hoare logic (apRHL) is a logic for formal verification of the differential privacy of databases written in the programming language pWHILE. Strictly speaking, however, this logic deals only with discrete random samplings. In this paper, we define the graded relational lifting of the subprobabilistic variant of Giry monad, which described differential privacy. We extend the logic apRHL with this graded lifting to deal with continuous random samplings. We give a generic method to give proof rules of apRHL for continuous random samplings.

Keywords: Differential privacy, Giry monad, graded monad, relational lifting, semantics,

1 Introduction

Differential privacy is a *definition* of privacy of *randomized* databases proposed by Dwork, McSherry, Nissim and Smith [7]. A randomized database satisfies ε -differential privacy (written ε -differentially private) if for any two adjacent data, the difference of their output probability distributions is bounded by the privacy strength ε . Differential privacy guarantees high secrecy against database attacks regardless of the attackers' background knowledge, and it has the composition laws, with which we can calculate the privacy strength of a composite database from the privacy strengths of its components.

Approximate relational Hoare logic (apRHL) [2,16] is a probabilistic variant of the *relational Hoare logic* [4] for formal verification of the differential privacy of databases written in the programming language pWHILE. In the logic apRHL, a parametric relational lifting, which relate probability distributions, play a central role to describe differential privacy in the framework of verification. This parametric lifting is an extension of the relational lifting [10, Section 3] that captures probabilistic bisimilarity of Markov chains [13] (see also [6, lemma 4]). The concept

¹ Email: satoutet@kurims.kyoto-u.ac.jp

of differential privacy is described in the category of binary relation and mappings between them, and verified by the logic apRHL.

Strictly speaking, however, apRHL deals only with random samplings of *discrete* distributions, while the algorithms in many actual studies for differential privacy are modelled with *continuous* distributions, such as, the Laplacian distributions over real line. Therefore apRHL is desired to be extended to deal with random continuous samplings.

1.1 Contributions

Main contributions of this paper are the following two points:

- We define the graded relational lifting of sub-Giry monad describing differential privacy for continuous random samplings.
- We extend the logic apRHL [2,16] for continuous random samplings (we name *continuous apRHL*).

This graded relational lifting is developed without witness distributions of probabilistic coupling, and hence is constructed in a different way from the coupling-based parametric lifting of relations given in the studies of apRHL [1,2,16].

In the continuous apRHL, we mainly extend the proof rules for relation compositions and the frame rule. We also develop a generic method to construct proof rules for random samplings. By importing the new rules added to apRHL+ in [1], we give a formal proof of the differential privacy of the *above-threshold algorithm* for real-valued queries [8, Section 3.6].

1.2 Preliminaries

We denote by **Meas** the category of measurable spaces and measurable functions between them and denote by **Set** the category of all sets and functions. The category **Meas** is complete and cocomplete, and the forgetful functor $U: \mathbf{Meas} \rightarrow \mathbf{Set}$ preserves products and coproducts. We also denote by $\omega\mathbf{CPO}_\perp$ of the category of ω -complete partial orders with the least element and continuous functions.

A Category of Relations between Measurable Spaces

We introduce the category **BRel(Meas)** of binary relations between measurable spaces as follows:

- An object is a triple (X, Y, Φ) consisting of measurable spaces X and Y and a relation R between X and Y (i.e. $R \subseteq UX \times UY$). We remark that R does not need to be a measurable subset of the product space $X \times Y$.
- An arrow $(f, g): (X, Y, \Phi) \rightarrow (X', Y', \Phi')$ is a pair of measurable functions $f: X \rightarrow X'$ and $g: Y \rightarrow Y'$ such that $(Uf \times Ug)(\Phi) \subseteq \Phi'$.

When we write an object (X, Y, Φ) in **BRel(Meas)**, we omit writing the underlying spaces X and Y if they are obvious from the context. We write p for the forgetful functor $p: \mathbf{BRel}(\mathbf{Meas}) \rightarrow \mathbf{Meas} \times \mathbf{Meas}$ which extracting underlying spaces: $(X, Y, \Phi) \mapsto (X, Y)$. We call an endofunctor F on **BRel(Meas)** a *relational lifting* of an endofunctor E on **Meas** if $(E \times E)p = pF$.

The Sub-Giry Monad

The Giry monad on **Meas** is introduced in [9] to give a categorical approach to probability theory; each arrow $X \rightarrow Y$ in the Kleisli category of the Giry monad bijectively corresponds to a probabilistic transition from X to Y , and the Chapman-Kolmogorov equation corresponds to the associativity law of the Giry monad.

We recall the sub-probabilistic variant of the Giry monad, which we call the *sub-Giry monad* (see also [17, Section 4]):

- For any measurable space (X, Σ_X) , the measurable space $(\mathcal{G}X, \Sigma_{\mathcal{G}X})$ is defined as follows: the underlying set $\mathcal{G}X$ is the set of subprobability measures over X , and the σ -algebra $\Sigma_{\mathcal{G}X}$ is the coarsest one that makes the evaluation function $\text{ev}_A: \mathcal{G}X \rightarrow [0, 1]$ (mapping ν to $\nu(A)$) measurable for each $A \in \Sigma_X$.
- For each $f: X \rightarrow Y$ in **Meas**, $\mathcal{G}f: \mathcal{G}X \rightarrow \mathcal{G}Y$ is defined by $(\mathcal{G}f)(\nu) = \nu(f^{-1}(-))$.
- The unit η is defined by $\eta_X(x) = \delta_x$, where δ_x is the *Dirac measure* centred on x .
- The multiplication μ is defined by $\mu_X(\Xi)(A) = \int_{\mathcal{G}X} \text{ev}_A d(\Xi)$. The Kleisli lifting of $f: X \rightarrow \mathcal{G}Y$ is given by $f^\sharp(\nu)(A) = \int_X f(-)(A) d\nu$ ($\nu \in \mathcal{G}X$).

The monad \mathcal{G} is commutative strong with respect to the cartesian product in **Meas**. The strength $\text{st}_{-,=}: (-) \times \mathcal{G}(=) \Rightarrow \mathcal{G}(- \times =)$ is given by the product measure $\text{st}_{X,Y}(x, \nu) = \delta_x \otimes \nu$. The commutativity of \mathcal{G} is given from the Fubini theorem. The double strength $\text{dst}_{-,=}: \mathcal{G}(-) \times \mathcal{G}(=) \Rightarrow \mathcal{G}(- \times =)$ is given by $\text{dst}_{X,Y}(\nu_1, \nu_2) = \nu_1 \otimes \nu_2$.

The Kleisli category **Meas \mathcal{G}** is often called the category **SRel** of *stochastic relations* [17, Section 3]. The category **SRel** is $\omega\mathbf{CPO}_\perp$ -enriched (with respect to the cartesian monoidal structure) with the following pointwise order:

$$f \sqsubseteq g \iff \forall x \in X, B \in \Sigma_Y. f(x)(B) \leq g(x)(B) \quad (f, g: X \rightarrow Y \text{ in } \mathbf{SRel}).$$

The *least upper bound* $\sup_{n \in \mathbb{N}} f_n$ of any ω -chain $f_0 \sqsubseteq f_1 \sqsubseteq \dots \sqsubseteq f_n \sqsubseteq \dots$ is given by $(\sup_n f_n)(x)(B) = \sup_n (f_n(x)(B))$. The *least function* of each **SRel**(X, Y) (written $\perp_{X,Y}$) is the constant function of the null-measure over Y . The *continuity* of composition is obtained from the following two facts:

- From the definition of Lebesgue integral, for any ω -chain $\{\nu_n\}$ of subprobability measures over X , $\int_X f d(\sup_n \nu_n) = \sup_n \int_X f d\nu_n$ holds.
- From the monotone convergence theorem, we have $\int_X \sup_n f_n d\nu = \sup_n \int_X f_n d\nu$.

This enrichment is equivalent to the partially additive structure on **SRel** [17, Section 5]: For any ω -chain $\{f_n\}_{n \in \mathbb{N}}$ of $f_n: X \rightarrow Y$ in **SRel**, we have the summable sequence $\{g_n\}_n$ where $g_0 = f_0$ and $g_{n+1} = f_{n+1} - f_n$. Conversely, for any summable sequence $\{g_n\}_{n \in \mathbb{N}}$, the functions $f_n = \sum_{k=0}^n g_k$ form an ω -chain.

Differential privacy

Throughout this paper, we define the approximate differential privacy as follows:

Definition 1.1 [[8, Definition 2.4], Modified] A measurable function $c: \mathbb{R}^m \rightarrow \mathcal{G}(\mathbb{R}^n)$ is (ε, δ) -differentially private if $c(x)(A) \leq \exp(\varepsilon)c(y)(A) + \delta$ holds for any $\|x - y\|_1 \leq 1$ and $A \in \Sigma_{\mathbb{R}^n}$, where $\|\cdot\|_1$ is 1-norm of the Euclidean space \mathbb{R}^m .

What we modify from the original definition [8, Definition 2.4] is the domain and codomain of c ; we replace the domain from \mathbb{N} to \mathbb{R} , and replace the codomain from a discrete probability space to $\mathcal{G}(\mathbb{R}^n)$. We apply this definition to the interpretation of pWHILE programs. The input and output spaces can be other spaces: in section 4 we consider the *above-threshold algorithm* **Above** whose output space is \mathbb{Z} . The above modification is essential in describing and verifying the differential privacy of this algorithm because it takes a sample from Laplace distribution over *real line*.

2 A Graded Monad for Differential Privacy

The composition law of differential privacy plays crucial role to in the compositional verification of the differential privacy of database programs. Barthe, Köpf, Olmedo, and Zanella-Béguelin constructed a *parametric relational lifting* describing differential privacy, and developed a framework for compositional verification of differential privacy [2].

Following this relational approach, we construct the parametric relational lifting of Giry monad to describe differential privacy for continuous random samplings. This lifting forms a graded monad on the category **BRel(Meas)** in the sense of [11]. The axioms of graded monad correspond to the (sequential) composition law of differential privacy.

2.1 Graded Monads

Definition 2.1 [11, Definition 2.2-bis] Let \mathbb{C} be a category, and $(M, \cdot, 1, \preceq)$ be a *preordered monoid*. An M -graded (or M -parametric effect) monad on \mathbb{C} consists of

- a collection $\{T_e\}_{e \in M}$ of endofunctors on \mathbb{C} ,
- a natural transformation $\eta: \text{Id} \Rightarrow T_1$,
- a collection $\{\mu^{e_1, e_2}\}_{e_1, e_2 \in M}$ of natural transformations $\mu^{e_1, e_2}: T_{e_1} T_{e_2} \Rightarrow T_{e_1 e_2}$,
- a collection $\{\sqsubseteq^{e_1, e_2}\}_{e_1 \preceq e_2}$ of natural transformations $\sqsubseteq^{e_1, e_2}: T_{e_1} \Rightarrow T_{e_2}$

satisfying

- $\mu^{e, 1} \circ T_e \eta = \mu^{1, e} \circ \eta_{T_e} = \text{Id}_{T_e}$ for any $e \in M$,
- $\mu^{(e_1 e_2), e_3} \circ \mu^{e_1, e_2} T_{e_3} = \mu^{e_1, (e_2, e_3)} \circ T_{e_1} \mu^{e_2, e_3}$ for all $e_1, e_2, e_3 \in M$,
- $\sqsubseteq^{e, e} = \text{Id}_{T_e}$ for any e and $\sqsubseteq^{e_2, e_3} \circ \sqsubseteq^{e_1, e_2} = \sqsubseteq^{e_1, e_3}$ whenever $e_1 \preceq e_2 \preceq e_3$,
- $\sqsubseteq^{(e_1 e_2), (e_3 e_4)} \circ \mu^{e_1, e_2} = \mu^{e_3, e_4} \circ (\sqsubseteq^{e_1, e_3} * \sqsubseteq^{e_2, e_4})$ whenever $e_1 \preceq e_3$ and $e_2 \preceq e_4$.

An M -graded monad $(\{T_e\}_{e \in M}, \eta, \mu^{e_1, e_2}, \sqsubseteq^{e_1, e_2})$ on \mathbb{C} is called an M -graded lifting of monad (T, η^T, μ^T) on \mathbb{D} along $U: \mathbb{C} \rightarrow \mathbb{D}$ if $UT_e = TU$, $U(\eta) = \eta^T U$, $U(\mu^{e_1, e_2}) = \mu^T U$, and $U(\sqsubseteq^{e_1, e_2}) = \text{id}_T$.

2.2 A Graded Relational Lifting of Giry Monad for Differential Privacy

Let M be the cartesian product of the monoids $([1, \infty), \times, 1)$ and $([0, \infty), +, 0)$ equipped with the product order of numerical orders. For each $(\gamma, \delta) \in M$, we

define the following mapping of $\mathbf{BRel}(\mathbf{Meas})$ -objects by

$$\mathcal{G}^{(\gamma, \delta)} \Phi = \left\{ (\nu_1, \nu_2) \in \mathcal{G}X \times \mathcal{G}Y \left| \begin{array}{l} \forall A \in \Sigma_X, B \in \Sigma_Y. \\ \Phi(A) \subseteq B \implies \nu_1(A) \leq \gamma \nu_2(B) + \delta \end{array} \right. \right\}.$$

Proposition 2.2 $\{\mathcal{G}^{(\gamma, \delta)}\}_{(\gamma, \delta) \in M}$ forms an M -graded lifting of the monad $(\mathcal{G} \times \mathcal{G}, \eta \times \eta, \mu \times \mu)$ along the forgetful functor $p: \mathbf{BRel}(\mathbf{Meas}) \rightarrow \mathbf{Meas} \times \mathbf{Meas}$.

Proof. Since the functor p is faithful, it suffices to show:

- (i) Each $\mathcal{G}^{(\gamma, \delta)}$ is an endofunctor on $\mathbf{BRel}(\mathbf{Meas})$.
- (ii) $(\text{id}_{\mathcal{G}X}, \text{id}_{\mathcal{G}Y})$ is an arrow $\mathcal{G}^{(\gamma, \delta)} \Phi \rightarrow \mathcal{G}^{(\gamma', \delta')} \Phi$ in $\mathbf{BRel}(\mathbf{Meas})$ for all $\gamma, \gamma', \delta, \delta'$ such that $\gamma \leq \gamma'$ and $\delta \leq \delta'$.
- (iii) (η_X, η_Y) is an arrow $\Phi \rightarrow \mathcal{G}^{(1, 0)} \Phi$ in $\mathbf{BRel}(\mathbf{Meas})$.
- (iv) (μ_X, μ_Y) is an arrow $\mathcal{G}^{(\gamma, \delta)} \mathcal{G}^{(\gamma', \delta')} \Phi \rightarrow \mathcal{G}^{(\gamma\gamma', \delta+\delta')} \Phi$ in $\mathbf{BRel}(\mathbf{Meas})$ for all $\gamma, \gamma', \delta, \delta'$.
- (i) Since the mapping $(f, g) \mapsto (\mathcal{G}f, \mathcal{G}g)$ is obviously functorial, it suffices to check that $(\mathcal{G}f, \mathcal{G}g)$ is an arrow $\mathcal{G}^{(\gamma, \delta)} \Psi \rightarrow \mathcal{G}^{(\gamma, \delta)} \Phi$ in $\mathbf{BRel}(\mathbf{Meas})$ for any arrow $(f, g): \Psi \rightarrow \Phi$ in $\mathbf{BRel}(\mathbf{Meas})$. This is proved from $\Phi(A) \subseteq B \implies \Psi(f^{-1}(A)) \subseteq g^{-1}(B)$ for any $A \in \Sigma_X$ and $B \in \Sigma_Y$. (ii) Obvious. (iii) Obvious. (iv) It suffices to show $(\mu_X \times \mu_Y)(\mathcal{G}^{(\gamma, \delta)} \mathcal{G}^{(\gamma', \delta')} \Phi) \subseteq \mathcal{G}^{(\gamma\gamma', \delta+\delta')} \Phi$ for any $\Phi \subseteq X \times Y$.

First, the following equation holds:

$$\mathcal{G}^{(\gamma, \delta)} \Phi = \left\{ (\nu_1, \nu_2) \left| \forall (f, g): \Phi \rightarrow \leq \text{ in } \mathbf{BRel}(\mathbf{Meas}). \int_X f \, d\nu_1 \leq \gamma \int_Y g \, d\nu_2 + \delta \right. \right\},$$

where \leq is the numerical order relation on $\mathcal{G}1 \simeq [0, 1]$. We omit the proof of this equation. It can be shown in the same way as [12, Theorem 12].

Let $(\Xi_1, \Xi_2) \in \mathcal{G}^{(\gamma, \delta)} \mathcal{G}^{(\gamma', \delta')} \Phi$. Assume $\Phi(A) \subseteq B$. We give $(f, g): \mathcal{G}^{(\gamma', \delta')} \Phi \rightarrow \leq$ in $\mathbf{BRel}(\mathbf{Meas})$ by $f = \max(\text{ev}_A - \delta', 0)$ and $g = \min(\gamma' \cdot \text{ev}_B, 1)$. They actually satisfy $f(\nu_1) \leq g(\nu_2)$ for each $(\nu_1, \nu_2) \in \mathcal{G}^{(\gamma', \delta')} \Phi$. Hence,

$$\begin{aligned} \mu_X(\Xi_1)(A) - \delta' &\leq \int_{\mathcal{G}X} (\text{ev}_A - \delta') \, d\Xi_1 \leq \int_{\mathcal{G}X} f \, d\Xi_1 \\ &\leq \gamma \int_{\mathcal{G}X} g \, d\Xi_2 + \delta \leq \gamma \int_{\mathcal{G}X} \gamma' \text{ev}_B \, d\Xi_2 + \delta = \gamma\gamma' \mu_Y(\Xi_2)(B) + \delta. \end{aligned}$$

This implies $\mu_X(\Xi_1)(A) \leq \gamma\gamma' \mu_Y(\Xi_2)(B) + \delta + \delta'$. \square

The M -graded lifting $\{\mathcal{G}^{(\gamma, \delta)}\}_{(\gamma, \delta) \in M}$ describes only one side of inequalities in the definition of differential privacy. By symmetrising this, we obtain the following M -graded lifting $\{\overline{\mathcal{G}}^{(\gamma, \delta)}\}_{(\gamma, \delta) \in M}$ exactly describing the differential privacy for continuous probabilities:

$$\overline{\mathcal{G}}^{(\gamma, \delta)} = \mathcal{G}^{(\gamma, \delta)}(-) \cap (\mathcal{G}^{(\gamma, \delta)}(-)^{\mathfrak{P}})^{\mathfrak{P}}.$$

Theorem 2.3 *A measurable function $c: \mathbb{R}^m \rightarrow \mathcal{G}(\mathbb{R}^n)$ is (ε, δ) -differentially private if and only if (c, c) is an arrow $\{ (x, y) \mid \|x - y\|_1 \leq 1 \} \rightarrow \overline{\mathcal{G}^{(\exp(\varepsilon), \delta)}} \text{Eq}_{\mathbb{R}^n}$ in $\mathbf{BRel}(\mathbf{Meas})$.*

In the original works [2, 3] of apRHL, the following relational lifting $(-)^{\sharp(\gamma, \delta)}$ is introduced to describe differential privacy. This lifting relates two distributions if there are intermediate distributions d_1 and d_R , called *witnesses*, whose skew distance, defined by $\Delta_\gamma^X(d_L, d_R) = \sup_{C \subseteq X} \{|d_L(C) - \gamma d_R(C)|, |d_R(C) - \gamma d_L(C)|\}$, is less than or equal to δ .

Definition 2.4 ([3, Definition 4], [16, Definition 4.3] and [1, Definition 8]) We denote by \mathcal{D} the subdistribution monad over \mathbf{Set} . Let Ψ be a relation between sets X and Y , and $d_1 \in \mathcal{D}X$ and $d_2 \in \mathcal{D}Y$ be two subdistributions. We define the relation $\Psi^{\sharp(\gamma, \delta)} \subseteq \mathcal{D}X \times \mathcal{D}Y$ as follows: $(d_1, d_2) \in \Psi^{\sharp(\gamma, \delta)}$ if and only if there are two subdistributions $d_L, d_R \in \mathcal{D}(X \times Y)$, called *witnesses*, such that

$$\mathcal{D}\pi_1(d_L) = d_1, \mathcal{D}\pi_2(d_R) = d_2, \text{supp}(d_L) \subseteq \Psi, \text{supp}(d_R) \subseteq \Psi, \Delta_\gamma^{X \times Y}(d_L, d_R) \leq \delta.$$

Proposition 2.5 *For any countable discrete spaces X and Y , and relation $\Psi \subseteq X \times Y$, we have $\Psi^{\sharp(\gamma, \delta)} \subseteq \overline{\mathcal{G}^{(\gamma, \delta)}}\Psi$.*

Proof. Suppose $(d_1, d_2) \in \Psi^{\sharp(\gamma, \delta)}$ with witnesses d_L and d_R . For any $A \subseteq X$, since $\text{supp}(d_L) \subseteq \Psi$ and $(A \times Y) \cap \Psi \subseteq X \times \Psi(A)$, we obtain:

$$\begin{aligned} d_1(A) &= \mathcal{D}\pi_1(d_L)(A) = d_L(A \times Y) = d_L((A \times Y) \cap \Psi) \leq d_L(X \times \Psi(A)) \\ &\leq \gamma d_R(X \times \Psi(A)) + \delta = \gamma \mathcal{D}\pi_2(d_R)(\Psi(A)) + \delta = \gamma d_2(\Psi(A)) + \delta. \end{aligned}$$

This implies $(d_1, d_2) \in \overline{\mathcal{G}^{(\gamma, \delta)}}\Psi$. Since the construction of $(-)^{\sharp(\gamma, \delta)}$ is symmetric, we conclude $(d_1, d_2) \in \overline{\mathcal{G}^{(\gamma, \delta)}}\Psi$. \square

We remark $\mathcal{G}X = \mathcal{D}X$ for countable discrete space X . When X is not countable, we have the above results by embedding each $d \in \mathcal{D}X$ in the set $\mathcal{D}X'$ of subprobability distributions over the countable *subspace* $X' = X \cap \text{supp}(d)$.

Corollary 2.6 *We have $\text{Eq}_X^{\sharp(\gamma, \delta)} = \overline{\mathcal{G}^{(\gamma, \delta)}}\text{Eq}_X$ for each countable discrete space X .*

Proof. (\subseteq) This inclusion is given from Proposition 2.5. (\supseteq) Suppose $(d_1, d_2) \in \overline{\mathcal{G}^{(\gamma, \delta)}}\text{Eq}_X$. This is equivalent to $\Delta_\gamma^X(d_1, d_2) \leq \delta$. Hence $(d_1, d_2) \in \text{Eq}_X^{\sharp(\gamma, \delta)}$ is proved by the witnesses given by $d_L = \sum_{x \in X} d_1(x) \cdot \delta_{(x, x)}$ and $d_R = \sum_{x \in X} d_2(x) \cdot \delta_{(x, x)}$. \square

3 The Continuous apRHL

We introduce a variant of the approximate probabilistic relational Hoare logic (apRHL) to deal with continuous random samplings. We name it the *continuous apRHL*.

3.1 The Language pWHILE

We recall and reformulate categorically the language pWHILE [2]. In this paper, we mainly refer to the categorical semantics of a probabilistic language given in [5,

Section 2]. The language pWHILE is constructed in the standard way, hence we sometimes omit the details of its construction.

3.1.1 Syntax

We introduce the syntax of pWHILE by the following BNF:

$$\begin{aligned}
\tau &::= \text{bool} \mid \text{int} \mid \text{real} \mid \dots \\
e &::= x \mid p(e_1, \dots, e_m) \\
\nu &::= d(e_1, \dots, e_m) \\
i &::= x \leftarrow e \mid x \stackrel{\$}{\leftarrow} \nu \mid \text{if } e \text{ then } c_1 \text{ else } c_2 \mid \text{while } e \text{ do } c \\
c &::= \text{skip} \mid \text{null} \mid \mathcal{I}; \mathcal{C}
\end{aligned}$$

Here, τ is a *value type*; x is a *variable*; p is an *operation*; d is a *probabilistic operation*; e is an *expression*; ν is a *probabilistic expression*; i is an *imperative*; c is a *command* (or program). We remark constants are 0-ary operations.

We introduce the following syntax sugars for simplicity:

$$\begin{aligned}
&\text{if } b \text{ then } c = \text{if } b \text{ then } c \text{ else skip} \\
[\text{while } b \text{ do } c]_n &= \begin{cases} \text{if } b \text{ then null else skip,} & \text{if } n = 0 \\ \text{if } b \text{ then } c; [\text{while } b \text{ do } c]_k, & \text{if } n = k + 1 \end{cases}
\end{aligned}$$

3.1.2 Typing Rules

We introduce a typing rule on the language pWHILE. A typing context is a finite set $\Gamma = \{x_1: \tau_1, x_2: \tau_2, \dots, x_n: \tau_n\}$ of pairs of a variable and a value type such that each variable occurs only once in the context.

We give typing rules of pWHILE as follows:

$$\begin{aligned}
&\frac{\Gamma \vdash^t e_1: \tau_1 \dots \Gamma \vdash^t e_n: \tau_n \quad p: (\tau_1, \dots, \tau_n) \rightarrow \tau}{\Gamma \vdash^t p(e_1, \dots, e_n): \tau} \quad \frac{\Gamma, x: \tau \vdash^t e: \tau}{\Gamma, x: \tau \vdash x \leftarrow e} \quad \frac{}{\Gamma \vdash \text{skip}} \\
&\frac{x: \tau \in \Gamma \quad \Gamma \vdash^t e_1: \tau_1 \dots \Gamma \vdash^t e_n: \tau_n \quad d: (\tau_1, \dots, \tau_n) \rightarrow \tau}{\Gamma \vdash x \stackrel{\$}{\leftarrow} d(e_1, \dots, e_n): \tau} \quad \frac{}{\Gamma \vdash \text{null}} \\
&\frac{\Gamma \vdash i \quad \Gamma \vdash c}{\Gamma \vdash i; c} \quad \frac{\Gamma \vdash^t b: \text{bool} \quad \Gamma \vdash c_1 \quad \Gamma \vdash c_2}{\Gamma \vdash \text{if } b \text{ then } c_1 \text{ else } c_2} \quad \frac{\Gamma \vdash^t b: \text{bool} \quad \Gamma \vdash c}{\Gamma \vdash \text{while } b \text{ do } c}
\end{aligned}$$

Here, the type $(\tau_1, \dots, \tau_n) \rightarrow \tau$ of each operation p and each probabilistic operation d are assumed to be given in advance.

We easily define inductively the set of free variables of commands, expressions, and probabilistic expressions (denoted by $FV(c)$, $FV(e)$, and $FV(\nu)$).

3.1.3 Denotational Semantics

We introduce a denotational semantics of pWHILE in **Meas**. We give the interpretations $\llbracket \tau \rrbracket$ of the value types τ :

- $\llbracket \text{bool} \rrbracket = \mathbb{B} = 1 + 1 = \{\text{true}, \text{false}\}$ (discrete space)
- $\llbracket \text{int} \rrbracket = \mathbb{Z}$ (discrete space)

- $\llbracket \text{real} \rrbracket = \mathbb{R}$ (Lebesgue measurable space)

We interpret a typing context $\Gamma = \{x_1 : \tau_1, x_2 : \tau_2, \dots, x_n : \tau_n\}$ as the product space $\llbracket \tau_1 \rrbracket \times \llbracket \tau_2 \rrbracket \times \dots \times \llbracket \tau_n \rrbracket$. We interpret each operation $p : (\tau_1, \dots, \tau_m) \rightarrow \tau$ as a measurable function $\llbracket p \rrbracket : \llbracket \tau_1 \rrbracket \times \dots \times \llbracket \tau_m \rrbracket \rightarrow \llbracket \tau \rrbracket$, and each probabilistic operation $d : (\tau_1, \dots, \tau_m) \rightarrow \tau$ as $\llbracket d \rrbracket : \llbracket \tau_1 \rrbracket \times \dots \times \llbracket \tau_m \rrbracket \rightarrow \mathcal{G}[\llbracket \tau \rrbracket]$. Typed terms $\Gamma \vdash^t e : \tau$ and commands $\Gamma \vdash c$ are interpreted to measurable functions of the forms $\llbracket \Gamma \rrbracket \rightarrow \llbracket \tau \rrbracket$ and $\llbracket \Gamma \rrbracket \rightarrow \mathcal{G}[\llbracket \Gamma \rrbracket]$ respectively.

The interpretation of expressions are defined inductively by:

$$\llbracket \Gamma \vdash^t x : \tau \rrbracket = \pi_{x : \tau} \quad \llbracket \Gamma \vdash^t p(e_1, \dots, e_m) \rrbracket = \llbracket p \rrbracket(\llbracket \Gamma \vdash^t e_1 \rrbracket, \dots, \llbracket \Gamma \vdash^t e_m \rrbracket)$$

The interpretation of commands are defined inductively by:

$$\begin{aligned} \llbracket \Gamma \vdash \text{skip} \rrbracket &= \eta_{\llbracket \Gamma \rrbracket} \quad \llbracket \Gamma \vdash \text{null} \rrbracket = \perp_{\llbracket \Gamma \rrbracket, \llbracket \Gamma \rrbracket} \quad \llbracket \Gamma \vdash i; c \rrbracket = (\llbracket \Gamma \vdash c \rrbracket)^\# \circ \llbracket \Gamma \vdash i \rrbracket \\ \llbracket \Gamma \vdash x \stackrel{\$}{\leftarrow} d(e_1, \dots, e_m) \rrbracket &= \mathcal{G}(\rho_{(x : \tau, \Gamma)}) \circ \text{st}_{\llbracket \tau \rrbracket, \llbracket \Gamma \rrbracket} \circ \langle \llbracket d \rrbracket(\llbracket \Gamma \vdash^t e_1 \rrbracket, \dots, \llbracket \Gamma \vdash^t e_m \rrbracket), \text{id}_{\llbracket \Gamma \rrbracket} \rangle \\ \llbracket \Gamma, x : \tau \vdash x \leftarrow e \rrbracket &= \eta_{\llbracket \Gamma, x : \tau \rrbracket} \circ \rho_{(x : \tau, \Gamma)} \circ \langle \llbracket \Gamma, x : \tau \vdash e \rrbracket, \text{id}_{\llbracket \Gamma, x : \tau \rrbracket} \rangle \\ \llbracket \Gamma \vdash \text{if } b \text{ then } c_1 \text{ else } c_2 \rrbracket &= (\llbracket \Gamma \vdash c_1 \rrbracket, \llbracket \Gamma \vdash c_2 \rrbracket) \circ \cong_{\llbracket \Gamma \rrbracket} \circ \langle \llbracket \Gamma \vdash b \rrbracket, \text{id}_{\llbracket \Gamma \rrbracket} \rangle \\ \llbracket \Gamma \vdash \text{while } b \text{ do } c \rrbracket &= \sup_{n \in \mathbb{N}} \llbracket \Gamma \vdash [\text{while } e \text{ do } c]_n \rrbracket \end{aligned}$$

Here,

- $\rho_{(x_k : \tau_k, \Gamma)} = \langle f_l \rangle_{l \in \{1, 2, \dots, n\}} : \llbracket \tau_k \rrbracket \times \llbracket \Gamma \rrbracket \rightarrow \llbracket \Gamma \rrbracket$, where $\Gamma = \{x_1 : \tau_1, x_2 : \tau_2, \dots, x_n : \tau_n\}$, $f_k = \pi_2$, and $f_l = \pi_l \circ \pi_2$ ($l \neq k$).
- $\cong_X : 2 \times X \rightarrow X + X$ is the inverse of $[\langle \iota_1 \circ !_X, \text{id} \rangle, \langle \iota_2 \circ !_X, \text{id} \rangle] : X + X \rightarrow 2 \times X$, which is obtained from the distributivity of the category **Meas**.

We remark that, from the commutativity of the monad \mathcal{G} , if $\Gamma \vdash x : \tau$ and $x \notin FV(c)$ then $\llbracket \Gamma \vdash c \rrbracket \cong \text{dst}_{\llbracket \Gamma' \rrbracket, \llbracket \tau \rrbracket}(\llbracket \Gamma' \vdash c \rrbracket \times \eta_{\llbracket \tau \rrbracket})$ where $\Gamma' = \Gamma \setminus \{x : \tau\}$.

3.2 Judgements of apRHL

A judgement of apRHL is

$$c_1 \sim_{\gamma, \delta} c_2 : \Psi \Rightarrow \Phi,$$

where c_1 and c_2 are commands, and Ψ and Φ are objects in **BRel(Meas)**. We call the relations Ψ and Φ the *precondition* and *postcondition* of the judgement respectively. Inspired from the validity of asymmetric apRHL [2], we introduce the validity of the judgement of apRHL.

Definition 3.1 Let Ψ and Φ be relations over the space $\llbracket \Gamma \rrbracket$. A judgement $c_1 \sim_{\gamma, \delta} c_2 : \Psi \Rightarrow \Phi$ is valid (written $\models c_1 \sim_{\gamma, \delta} c_2 : \Psi \Rightarrow \Phi$) when $(\llbracket \Gamma \vdash c_1 \rrbracket, \llbracket \Gamma \vdash c_2 \rrbracket)$ is an arrow $\Psi \rightarrow \overline{\mathcal{G}^{(\gamma, \delta)}}\Phi$ in **BRel(Meas)**.

We often write preconditions and postconditions in the following manner: Let $\Gamma = \{x_1 : \tau_1, x_2 : \tau_2, \dots, x_n : \tau_n\}$. Assume $\Gamma \vdash e_1 : \tau$ and $\Gamma \vdash e_2 : \tau$, and let R be a relation on $\llbracket \tau \rrbracket$ (e.g. $=, \leq, \dots$). We define the relation $e_1 \langle 1 \rangle R e_2 \langle 2 \rangle$ on $\llbracket \Gamma \rrbracket$ by

$$(e_1 \langle 1 \rangle R e_2 \langle 2 \rangle) = \{ (m_1, m_2) \in \llbracket \Gamma \rrbracket \mid \llbracket \Gamma \vdash e_1 \rrbracket(m_1) R \llbracket \Gamma \vdash e_2 \rrbracket(m_2) \}.$$

3.3 Proof Rules

We mainly refer the proof rules of apRHL from [2,16], but we modify the [comp] and [frame] rules to verify differential privacy for continuous random samplings.

$$\begin{array}{c}
\frac{x_1 : \tau_1, x_2 : \tau_2 \in \Gamma \quad \Gamma \vdash^t e_1 : \tau_1 \quad \Gamma \vdash^t e_2 : \tau_2 \quad (\rho_{(x_1 : \tau_1, \Gamma)} \circ \langle \llbracket e_1 \rrbracket, \text{id} \rangle, \rho_{(x_2 : \tau_2, \Gamma)} \circ \langle \llbracket e_2 \rrbracket, \text{id} \rangle) : \Psi \rightarrow \Phi}{\models x_1 \leftarrow e_1 \sim_{(1,0)} x_2 \leftarrow e_2 : \Psi \Rightarrow \Phi} [\text{assn}] \\
\\
\frac{\Gamma \vdash^t e_1^1 : \tau \dots \Gamma \vdash^t e_m^1 : \tau \quad \Gamma \vdash^t e_1^2 : \tau \dots \Gamma \vdash^t e_m^2 : \tau \quad x_1 : \tau, x_2 : \tau \in \Gamma \quad d : (\tau_1, \dots, \tau_m) \rightarrow \tau \quad (\llbracket d \rrbracket, \llbracket d \rrbracket) : \Psi \rightarrow \overline{\mathcal{G}^{(\gamma, \delta)}}(\text{Eq}_{\llbracket \tau \rrbracket}) \text{ in } \mathbf{BRel}(\mathbf{Meas})}{\models x_1 \stackrel{\$}{\leftarrow} d(e_1^1, \dots, e_m^1) \sim_{(\gamma, \delta)} x_2 \stackrel{\$}{\leftarrow} d(e_1^2, \dots, e_m^2) : \Psi' \Rightarrow (x_1 \langle 1 \rangle = x_2 \langle 1 \rangle)} [\text{rand}] \\
\text{where } \Psi' = \{ ((g, a), (h, b)) \mid (a, b) \in \Psi, g, h \in \Gamma' \} \ (\Gamma = \{x_1 : \tau_1, \dots, x_k : \tau_k\} \cup \Gamma'). \\
\\
\frac{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \Rightarrow \Phi' \quad \models c'_1 \sim_{(\gamma', \delta')} c'_2 : \Phi' \Rightarrow \Phi \quad \models \text{skip} \sim_{(1,0)} \text{skip} : \Phi \Rightarrow \Phi}{\models c_1; c'_1 \sim_{(\gamma\gamma', \delta+\delta')} c_2; c'_2 : \Psi \Rightarrow \Phi} [\text{seq}] \quad \frac{}{\models \text{skip} \sim_{(1,0)} \text{skip} : \Phi \Rightarrow \Phi} [\text{skip}] \\
\\
\frac{\Gamma \vdash^t b : \text{bool} \quad \Gamma \vdash^t b : \text{bool} \quad \Psi \Rightarrow b \langle 1 \rangle = b' \langle 2 \rangle \quad \models c_1 \sim_{(\gamma, \delta)} c'_1 : \Psi \wedge b \langle 1 \rangle \Rightarrow \Phi \quad \models c_2 \sim_{(\gamma, \delta)} c'_2 : \Psi \wedge \neg b \langle 1 \rangle \Rightarrow \Phi}{\models \text{if } b \text{ then } c_1 \text{ else } c_2 \sim_{(\gamma, \delta)} \text{if } b' \text{ then } c'_1 \text{ else } c'_2 : \Psi \Rightarrow \Phi} [\text{cond}] \\
\\
\frac{\Gamma \vdash^t e : \text{int} \quad \gamma = \prod_{k=0}^{n-1} \gamma_k \quad \delta = \sum_{k=0}^{n-1} \delta_k \quad \Theta \Rightarrow b_1 \langle 1 \rangle = b_2 \langle 2 \rangle \quad \Theta \wedge e \langle 1 \rangle \geq n \Rightarrow \neg b_1 \langle 1 \rangle \quad \forall k : \text{int}. \models c_1 \sim_{(\gamma_k, \delta_k)} c_2 : \Theta \wedge e \langle 1 \rangle = k \wedge e \langle 1 \rangle \leq n \implies \Theta \wedge e \langle 1 \rangle > k}{\models \text{while } b \text{ do } c_1 \sim_{(\gamma, \delta)} \text{while } b' \text{ do } c_2 : \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq 0 \Rightarrow \Theta \wedge \neg b_1 \langle 1 \rangle} [\text{while}] \\
\\
\frac{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \wedge \Theta \Rightarrow \Phi \quad \models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \wedge \neg \Theta \Rightarrow \Phi}{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \Rightarrow \Phi} [\text{case}] \\
\\
\frac{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \Rightarrow \Phi \quad \Psi' \Rightarrow \Psi \quad \Phi \Rightarrow \Phi'}{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi' \Rightarrow \Phi'} [\text{weak}] \quad \frac{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \Rightarrow \Phi}{\models c_2 \sim_{(\gamma, \delta)} c_1 : \Psi^\Phi \Rightarrow \Phi^\Phi} [\text{op}]
\end{array}$$

The relational lifting $\overline{\mathcal{G}^{(\gamma, \delta)}}$ does not preserve every relation composition. However, it preserve the composition of relations if the relations are *measurable*, that is, the images and inverse images along them of measurable sets are also measurable (see also [12, Section 3.3]). Generally speaking, it is difficult to check measurability of relations, hence the continuous apRHL is weak for dealing with relation compositions. However, we have the following two special cases:

- The *equality/diagonal* relation on any space is a measurable relation.
- Any relation between *discrete* spaces is automatically a measurable relation.

Hence, the following [comp] rule is an extension of the original [comp] rule in [2]:

$$\frac{\begin{array}{c} \Phi \text{ and } \Phi' \text{ are measurable relations} \\ \models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \Rightarrow \Phi \quad \models c_2 \sim_{(\gamma', \delta')} c_3 : \Psi' \Rightarrow \Phi' \end{array}}{\models c_1 \sim_{(\gamma\gamma', \min(\delta+\gamma\delta', \delta'+\gamma'\delta))} c_3 : \Psi \circ \Psi' \Rightarrow \Phi \circ \Phi'} [\text{comp}]$$

To define the [frame] rule in continuous apRHL, for any relation Θ on $\llbracket \Gamma \rrbracket$, we define the following relation $\text{Range}(\Theta)$:

$$\begin{aligned} & \text{Range}(\Theta) \\ &= \{ (\nu_1, \nu_2) \mid \exists A, B \in \Sigma_{\llbracket \Gamma \rrbracket}. (A \times B \subseteq \Theta \wedge \nu_1(A) = \nu_1(\llbracket \Gamma \rrbracket) \wedge \nu_2(B) = \nu_2(\llbracket \Gamma \rrbracket)) \}. \end{aligned}$$

We define the [frame] rule with the construction $\text{Range}(-)$:

$$\frac{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \Rightarrow \Phi \quad (\llbracket c_1 \rrbracket, \llbracket c_2 \rrbracket) : \Theta \rightarrow \text{Range}(\Theta)}{\models c_1 \sim_{(\gamma, \delta)} c_2 : \Psi \wedge \Theta \Rightarrow \Phi \wedge \Theta} [\text{frame}]$$

If $\llbracket \Gamma \rrbracket$ is countable discrete then the condition $(\nu_1, \nu_2) \in \text{Range}(\Theta)$ is equivalent to $\text{supp}(\nu_1) \times \text{supp}(\nu_2) \subseteq \Theta$, and hence the above [frame] rule is an extension of the original [frame] rule in [2].

Note that if the σ -algebra of the space $\llbracket \tau \rrbracket$ contains all singleton subsets, and Θ does not restrict any variables in $FV(c_1) \cup FV(c_2)$ then $(\llbracket c_1 \rrbracket, \llbracket c_2 \rrbracket) : \Theta \rightarrow \text{Range}(\Theta)$.

3.4 Soundness

The soundness of the [assn] and [case] are obtained from the composition of arrows in **BRel(Meas)**. The rule [skip] and [seq] are sound because $\overline{\mathcal{G}}^{(\gamma, \delta)}$ is the graded relational lifting of $\mathcal{G} \times \mathcal{G}$ along the forgetful functor $U : \mathbf{BRel}(\mathbf{Meas}) \rightarrow \mathbf{Meas}^2$. The rules [weak] and [op] are sound because $\overline{\mathcal{G}}^{(\gamma, \delta)}$ is monotone with respect to the inclusion order of relations, and preserves opposites of relations. The soundness of [rand] is proved from Fubini theorem. The soundness of [cond] is proved by case analyses. The soundness of [while] is obtained from $\omega\mathbf{CPO}_\perp$ -enrichment structure of **SRel**. The soundness of [comp] is given by using the measurability of the postconditions. Finally, the [frame] rule is proved from the structure of $\text{Range}(\Theta)$.

3.5 Mechanisms

In this part, we give a generic method to construct the rules for random samplings, and by instantiating the method we show the soundness of the proof rules in prior researches: [Lap] for Laplacian mechanism [7], [Exp] for Exponential mechanism [14], [Gauss] for Gaussian mechanism [8, Theorem 3.22, Theorem A.1], and [Cauchy] for the mechanism by Cauchy distributions [15].

Let $f : X \times Y \rightarrow \mathbb{R}$ be a positive measurable function, and ν be a measure over Y . We define the following function $f_a : \Sigma_Y \rightarrow [0, 1]$ by

$$f_a(B) = \frac{\int_B f(a, -) d\nu}{\int_Y f(a, -) d\nu}.$$

We remark that the function $f(a, -): Y \rightarrow \mathbb{R}$ is measurable. If the function is not ‘almost everywhere zero’ and Lebesgue integrable, that is, $0 < \int_Y f(a, -) d\nu < \infty$ then $f_a(-)$ is a *probability measure*.

The following proposition, which is an extension of [2, Lemma 7], plays the central role in the construction of sound proof rules for random samplings.

Proposition 3.2 *Let $f: X \times Y \rightarrow \mathbb{R}$ be a positive measurable function, and ν be a measure over Y . For all $a, a' \in X$, $\gamma, \gamma' \geq 1$, $\delta \geq 0$, and $Z \in \Sigma_Y$ (window set), if the following three conditions hold then for any $B \in \Sigma_Y$, we have $f_a(B) \leq \gamma\gamma'f_{a'}(B) + \delta$.*

- (i) $0 < \frac{1}{\gamma'} \int_Y f(a', -) d\nu \leq \int_Y f(a, -) d\nu < \infty$
- (ii) $\forall b \in Z. f(a, b) \leq \gamma f(a', b)$, (iii) $f_a(Y \setminus Z) \leq \delta$.

Laplacian mechanism [7].

We give the function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ by $f(a, b) = \frac{2}{\sigma} \exp(\frac{-|b-a|}{\sigma})$, where $\sigma > 0$ is the variance of Laplacian mechanism. We introduce the probabilistic operation $\text{Lap}_\sigma: \text{real} \rightarrow \text{real}$ with $\llbracket \text{Lap}_\sigma \rrbracket = f_{(-)}$, whose measurability is shown from the continuity of the mapping $a \mapsto \int_\alpha^\beta f(a, x) dx$ ($\alpha, \beta \in \mathbb{R}$).

We show $(f_{(-)}, f_{(-)}): \{ (a, a') \mid |a - a'| < r \} \rightarrow \overline{\mathcal{G}^{(\exp(\frac{r}{\sigma}), 0)}} \text{Eq}_{\mathbb{R}}$ by instantiating Proposition 3.2 as follows: If $|a - a'| < r$ then the following parameters satisfy the conditions (i)–(iii): $\gamma = \exp(r/\sigma)$, $\gamma' = 1$, $\delta = 0$, the function f , the Lebesgue measure ν over \mathbb{R} , and the window $Z = \mathbb{R}$. This implies $(f_{(-)}, f_{(-)}): \{ (a, a') \mid |a - a'| < r \} \rightarrow \overline{\mathcal{G}^{(\exp(\frac{r}{\sigma}), 0)}} \text{Eq}_{\mathbb{R}}$ since $\{ (a, a') \mid |a - a'| < r \}$ and $\text{Eq}_{\mathbb{R}}$ are symmetric.

From the [rand] rule, the following rule is proved:

$$\frac{\Gamma \vdash^t e_1: \text{real} \quad \Gamma \vdash^t e_2: \text{real} \quad m_1 \Psi m_2 \Rightarrow |\llbracket e_1 \rrbracket m_1 - \llbracket e_2 \rrbracket m_2| < r}{\models x \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e_1) \sim_{(\exp(\frac{r}{\sigma}), 0)} y \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e_2): \Psi \Rightarrow x\langle 1 \rangle = y\langle 2 \rangle} [\text{Lap}]$$

Exponential mechanism [14, Modified].

Let D be the discrete Euclidian space \mathbb{Z}^n , and (R, ν) be a (positive) measure space. Let $q: D \times R \rightarrow \mathbb{R}$ be a measurable function such that $\sup_{b \in R} |q(a, b) - q(a', b)| \leq c \cdot \|a - a'\|_1$ for some $c > 0$. Suppose $0 < \int_R \exp(\varepsilon q(a, -)) d\nu < \infty$ for any $a \in D$. We give the function $f: D \times R \rightarrow \mathbb{R}$ by $f(a, b) = \exp(\varepsilon q(a, b))$, where $\varepsilon > 0$ is a constant. We add the value types D and R with $\llbracket \mathsf{D} \rrbracket^\Gamma = D$ and $\llbracket \mathsf{R} \rrbracket^\Gamma = R$ to pWHILE, and introduce the probabilistic operation $\text{Exp}_{\langle q, \nu, \varepsilon \rangle}: \mathsf{D} \rightarrow \mathsf{R}$ with $\llbracket \text{Exp}_{\langle q, \nu, \varepsilon \rangle} \rrbracket = f_{(-)}$.

We show $(f_{(-)}, f_{(-)}): \{ (a, a') \mid \|a - a'\|_1 < r \} \rightarrow \overline{\mathcal{G}^{(\exp(2\varepsilon rc), 0)}} \text{Eq}_R$ by instantiating Proposition 3.2 as follows: Suppose $\|a - a'\|_1 < r$. The following parameters then satisfy the conditions (i)–(iii): $\gamma = \gamma' = \exp(\varepsilon rc)$, $\delta = 0$, the function f , the given measure ν , and the window $Z = R$.

From the [rand] rule, the following rule is proved:

$$\frac{\Gamma \vdash^t e_1: \mathsf{D} \quad \Gamma \vdash^t e_2: \mathsf{D} \quad m_1 \Psi m_2 \Rightarrow |\llbracket e_1 \rrbracket m_1 - \llbracket e_2 \rrbracket m_2\|_1 < r}{\models x \stackrel{\$}{\leftarrow} \text{Exp}_{\langle q, \nu, \varepsilon \rangle}(e_1) \sim_{(\exp(2\varepsilon rc), 0)} y \stackrel{\$}{\leftarrow} \text{Exp}_{\langle q, \nu, \varepsilon \rangle}(e_2): \Psi \Rightarrow x\langle 1 \rangle = y\langle 2 \rangle} [\text{Exp}]$$

Gaussian mechanism [8, Theorem 3.22, Theorem A.1].

We give the function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ by $f(a, b) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{(b-a)^2}{2\sigma^2})$, where $\sigma > 0$ is the variance of Gaussian mechanism. We introduce the probabilistic operation $\text{Gauss}_\sigma: \text{real} \rightarrow \text{real}$ with $\llbracket \text{Gauss}_\sigma \rrbracket = f_{(-)}$, whose continuity is easily proved.

We obtain $(f_{(-)}, f_{(-)}): \{ (a, a') \mid |a - a'| < r \} \rightarrow \overline{\mathcal{G}^{(\gamma, \delta)}} \text{Eq}_{\mathbb{R}}$ by instantiating Proposition 3.2 as follows: If $|a - a'| < r$, $1 < \gamma < \exp(1)$, and $\gamma' = 1$ hold, and there is $(3/2) < c$ such that $2\log(1.25/\delta) \leq c^2$ and $(cr/\log \gamma) \leq \sigma$, then the parameters γ , γ' , and δ , the function f , and the Lebesgue measure ν over \mathbb{R} satisfy the conditions (i)–(iii) for the window $Z = \{ b \mid |b - (a + a')/2| \leq (\sigma^2 \log \gamma / r) \}$.

From the [rand] rule, we obtain the following rule:

$$\frac{\begin{array}{l} \exists c > \frac{3}{2}. (2\log(\frac{1.25}{\delta}) < c^2 \ \wedge \ \frac{cr}{\gamma} \leq \sigma) \quad 1 < \gamma < \exp(1) \\ \Gamma \vdash^t e_1: \text{real} \quad \Gamma \vdash^t e_2: \text{real} \quad m_1 \Psi m_2 \Rightarrow |\llbracket e_1 \rrbracket m_1 - \llbracket e_2 \rrbracket m_2| < r \end{array}}{\vdash x \stackrel{\$}{\leftarrow} \text{Gauss}_\sigma(e_1) \sim_{(\gamma, \delta)} y \stackrel{\$}{\leftarrow} \text{Gauss}_\sigma(e_2): \Psi \Rightarrow x\langle 1 \rangle = y\langle 2 \rangle} [\text{Gauss}]$$

We can relax the above conditions for c to $((1 + \sqrt{3})/2) < c$ and $2\log(0.66/\delta) < c^2$ by changing the window Z to $\{ b \mid b \leq (a + a')/2 + (\sigma^2 \log \gamma / r) \}$ when $a \leq a'$ and $\{ b \mid b \geq (a + a')/2 - (\sigma^2 \log \gamma / r) \}$ when $a' \leq a$.

Mechanism of Cauchy distributions [15]

We give the function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ by $f(a, b) = \frac{\rho}{\pi((a-b)^2 + \rho^2)}$. We introduce the probabilistic operation $\text{Cauchy}_\rho: \text{real} \rightarrow \text{real}$ with $\llbracket \text{Cauchy}_\rho(e) \rrbracket^\Gamma m = f_{(-)}$, whose continuity is easily proved.

Let $\gamma = 1 + \frac{r^2 + r\sqrt{r^2 + 4\rho^2}}{2\rho^2}$. We obtain $(f_{(-)}, f_{(-)}): \{ (a, a') \mid |a - a'| < r \} \rightarrow \overline{\mathcal{G}^{(\gamma, 0)}} \text{Eq}_{\mathbb{R}}$ by instantiating Proposition 3.2 as follows: If $|a - a'| < r$ then the parameters satisfy the conditions (i)–(iii): γ , $\gamma' = 1$, $\delta = 0$, the Lebesgue measure ν over \mathbb{R} , and the window $Z = \mathbb{R}$.

From the [rand] rule, we obtain the following rule:

$$\frac{\Gamma \vdash^t e: \text{real} \quad m_1 \Psi m_2 \Rightarrow |\llbracket e_1 \rrbracket m_1 - \llbracket e_2 \rrbracket m_2| < r}{\vdash x \stackrel{\$}{\leftarrow} \text{Cauchy}_\rho(e_1) \sim_{(\gamma, 0)} y \stackrel{\$}{\leftarrow} \text{Cauchy}_\rho(e_2): \Psi \Rightarrow (\pi_x \times \pi_y)^{-1}(\text{Eq}_{\mathbb{R}})} [\text{Cauchy}]$$

4 An Example: The Above Threshold Algorithm

Barthe, Gaboardi, Grégoire, Hsu, and Strub extended the logic apRHL to the logic apRHL+ with new proof rules to describe the *sparse vector technique* (see also [8, Section 3.6]). They gave a formal proof of the differential privacy of *above threshold algorithm* in the preprint [1] in arXiv.

In this section, we demonstrate that the above threshold algorithm with *real-valued queries* is proved with *almost the same proof* as in [1]. The new proof rules of apRHL+ are still sound in the framework of the continuous apRHL.

We consider the following algorithm **AboveT**:

Algorithm 1 The Above Threshold Algorithm ([1], Modified)

```

1: AboveT( $T$ : real,  $Q$ : queries,  $d$ : data)
2:    $j \leftarrow 1$ ;  $r \leftarrow |Q| + 1$ ;  $T \stackrel{\$}{\leftarrow} \text{Lap}_{\varepsilon/2}(t)$ ;
3:   while  $j < |Q|$  do
4:      $S \stackrel{\$}{\leftarrow} \text{Lap}_{\varepsilon/4}(\text{eval}(Q, i, d))$ ;
5:     if  $T \leq S \wedge r = |Q| + 1$  then
6:        $r \leftarrow j$ ;
7:      $j \leftarrow j + 1$ 

```

We recall the setting of this algorithm. This algorithm has two fixed parameters: the threshold t : **real** and the set Q : **queries** of queries where $|Q|$: **int** is the number of Q . The input variable is d : **int**, and the output variable is r : **int**. We prepare the new value types **queries** and **data** with $\llbracket \text{data} \rrbracket = \mathbb{R}^N$ and **queries** = **int** (alias), and the typings j : **int**, T : **real**, and S : **real**. We assume that an operation $\text{eval}: (\text{queries}, \text{int}, \text{data}) \rightarrow \text{real}$ is given for evaluating i -th query in Q for the input d . We require $\llbracket \text{eval} \rrbracket$ to be 1-*sensitivity* for the data d , that is, $\|d - d'\|_1 \leq 1 \Rightarrow \|\llbracket \text{eval} \rrbracket(Q, i, d) - \llbracket \text{eval} \rrbracket(Q, i, d')\| \leq 1$.

The differential privacy of **Above** is characterised as follows:

$$\models \text{AboveT} \sim_{\exp(\varepsilon), 0} \text{AboveT}: \|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \Rightarrow r\langle 1 \rangle = r\langle 2 \rangle.$$

The following rules in apRHL+ are sound in the framework of continuous apRHL:

$$\frac{\forall i: \text{int}. \models c_1 \sim_{(\gamma, \delta_i)} c_2: \Psi \Rightarrow (x\langle 1 \rangle = i \Rightarrow x\langle 2 \rangle = i) \quad \sum_{i: \text{int}} \llbracket \delta_i \rrbracket = \delta}{\models c_1 \sim_{(\gamma, \delta)} c_2: \Psi \Rightarrow x\langle 1 \rangle = x\langle 2 \rangle} [\text{Forall-Eq}]$$

$$\frac{\Gamma \vdash^t e_1: \text{real} \quad \Gamma \vdash^t e_2: \text{real} \quad m_1 \Psi m_2 \Rightarrow \|\llbracket e_1 \rrbracket m_1 + r' - \llbracket e_2 \rrbracket m_2\| < r}{\models x \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e_1) \sim_{(\exp(\frac{r}{\sigma}), 0)} y \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e_2): \Psi \Rightarrow x\langle 1 \rangle + r' = y\langle 2 \rangle} [\text{LapGen}]$$

$$\frac{\Gamma \vdash^t e_1: \text{real} \quad \Gamma \vdash^t e_2: \text{real} \quad x \notin FV(e_1) \quad y \notin FV(e_2)}{\models x \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e_1) \sim_{(1, 0)} y \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e_2): \Psi \Rightarrow x\langle 1 \rangle - y\langle 2 \rangle = e_1\langle 1 \rangle - e_2\langle 2 \rangle} [\text{LapNull}]$$

Hence we extend the continuous apRHL by adding these rules, and therefore we construct a formal proof almost the same proof as in [1] in the extended continuous apRHL.

The soundness of the rule [Forall-Eq] is proved from the following lemma:

Lemma 4.1 ([1, Proposition 6], Modified) *If $x: \tau$ and the space $\llbracket \tau \rrbracket$ is countable discrete then*

$$\bigcap_{i \in \llbracket \tau \rrbracket} \mathcal{G}^{(\gamma, \delta_i)}(x\langle 1 \rangle = i \Rightarrow x\langle 2 \rangle = i) \subseteq \mathcal{G}^{(\gamma, \sum_{i \in \llbracket \tau \rrbracket} \delta_i)}(x\langle 1 \rangle = x\langle 2 \rangle).$$

The soundness of the rule [LapGen] is proved from the rules [Lap] and [assn] and the semantic equivalence $\llbracket x \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e + r'); x \leftarrow x - r' \rrbracket = \llbracket x \stackrel{\$}{\leftarrow} \text{Lap}_\sigma(e) \rrbracket$. The soundness of [LapNull] is proved by using the [LapGen] and [Frame] rules.

Formal Proof

We now demonstrate that the $(\varepsilon, 0)$ -differential privacy of algorithm **AboveT** is proved with almost the same proof as in [1].

From the [Forall-Eq] rule with variable r , it suffices to prove for all integer i ,

$$\models \mathbf{AboveT} \sim_{\exp(\varepsilon), 0} \mathbf{AboveT}: \|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \Rightarrow (r\langle 1 \rangle = i \Rightarrow r\langle 2 \rangle = i).$$

We denote by c_0 the sub-command consisting of the initialization line 2 of **AboveT**. From the rules [assn], [LapGen] rule with $r = r' = 1$, and $\sigma = 2/\varepsilon$, [seq], and [frame] we obtain

$$\models c_0 \sim_{\exp(\varepsilon/2), 0} c_0: \|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \Rightarrow \|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \wedge \Psi.$$

where

$$\Psi = T\langle 1 \rangle + 1 = T\langle 2 \rangle \wedge j\langle 1 \rangle = j\langle 2 \rangle \wedge j\langle 1 \rangle = 1 \wedge r\langle 1 \rangle = r\langle 2 \rangle \wedge r\langle 1 \rangle = |Q| + 1.$$

We denote by c_1 and c_2 the main loop and the body of the main loop respectively (i.e. $c_1 = \mathbf{while} (j < |Q|) \mathbf{do} c_2$). We aim to prove the following judgement by using the [while] rule:

$$\models c_1 \sim_{\exp(\varepsilon/2), 0} c_1: (\|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \wedge \Psi) \Rightarrow (r\langle 1 \rangle = i \Rightarrow r\langle 2 \rangle = i).$$

To prove this, it suffices to show the following cases for the loop body c_2 :

- (i) If $k < i$ then $\models c_2 \sim_{1, 0} c_2: (\Theta \wedge j\langle 1 \rangle = k) \Rightarrow (\Theta \wedge j\langle 1 \rangle > k)$
- (ii) If $k = i$ then $\models c_2 \sim_{\exp(\varepsilon/2), 0} c_2: (\Theta \wedge j\langle 1 \rangle = k) \Rightarrow (\Theta \wedge j\langle 1 \rangle > k)$
- (iii) If $k > i$ then $\models c_2 \sim_{1, 0} c_2: (\Theta \wedge j\langle 1 \rangle = k) \Rightarrow (\Theta \wedge j\langle 1 \rangle > k)$

Here, we provide the following *loop invariant* as follows:

$$\begin{aligned} \Theta = & (j\langle 1 \rangle < i \Rightarrow ((r\langle 1 \rangle = |Q| + 1 \Rightarrow r\langle 2 \rangle = |Q| + 1) \wedge (r\langle 1 \rangle = |Q| + 1 \vee r\langle 1 \rangle < i))) \\ & \wedge (j\langle 1 \rangle \geq i \Rightarrow (r\langle 1 \rangle = i \Rightarrow r\langle 2 \rangle = i)) \\ & \wedge \|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \wedge T\langle 1 \rangle + 1 = T\langle 2 \rangle \wedge j\langle 1 \rangle = j\langle 2 \rangle \end{aligned}$$

The judgement in the case (i) is proved from the rules [seq], [assn], [cond], and [frame] and the following fact obtained from the [LapNull] rule:

$$\begin{aligned} \models S \stackrel{\$}{\leftarrow} \mathbf{Lap}_{\varepsilon/4}(\mathbf{eval}(Q, i, d)) \sim_{1, 0} S \stackrel{\$}{\leftarrow} \mathbf{Lap}_{\varepsilon/4}(\mathbf{eval}(Q, i, d)): \\ (\|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1) \wedge (T\langle 1 \rangle + 1 = T\langle 2 \rangle) \Rightarrow ((S\langle 1 \rangle < T\langle 1 \rangle) \Rightarrow (S\langle 2 \rangle < T\langle 2 \rangle)). \end{aligned}$$

The case (ii) is proved from the rules [seq], [assn], [cond], and [frame] and the following fact obtained from the [LapGen] rule:

$$\begin{aligned} \models S \stackrel{\$}{\leftarrow} \mathbf{Lap}_{\varepsilon/4}(\mathbf{eval}(Q, i, d)) \sim_{\exp(\varepsilon/2), 0} S \stackrel{\$}{\leftarrow} \mathbf{Lap}_{\varepsilon/4}(\mathbf{eval}(Q, i, d)): \\ (\|d\langle 1 \rangle - d\langle 2 \rangle\|_1 \leq 1 \wedge T\langle 1 \rangle + 1 = T\langle 2 \rangle) \Rightarrow (S\langle 1 \rangle + 1 = S\langle 2 \rangle \wedge T\langle 1 \rangle + 1 = T\langle 2 \rangle). \end{aligned}$$

The case (iii) is proved in the similar way as (i).

Acknowledgement

The author thanks Shin-ya Katsumata for many valuable comments and stimulating discussions, Marco Gaboardi for helpful suggestions and the introduction of his preprint [1] in arXiv, Masahito Hasegawa, Naohiko Hoshino, and Takeo Uramoto for advices that contributed to improve the writing of this paper.

References

- [1] Gilles Barthe, Marco Gaboardi, Benjamin Grégoire, Justin Hsu, and Pierre-Yves Strub. Proving Differential Privacy via Probabilistic Couplings. *ArXiv e-prints*, January 2016.
- [2] Gilles Barthe, Boris Köpf, Federico Olmedo, and Santiago Zanella-Béguelin. Probabilistic relational reasoning for differential privacy. In *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '12, pages 97–110, New York, NY, USA, 2012. ACM.
- [3] Gilles Barthe and Federico Olmedo. Beyond differential privacy: Composition theorems and relational logic for f-divergences between probabilistic programs. In FedorV. Fomin, R?si?? Freivalds, Marta Kwiatkowska, and David Peleg, editors, *Automata, Languages, and Programming*, volume 7966 of *Lecture Notes in Computer Science*, pages 49–60. Springer Berlin Heidelberg, 2013.
- [4] Nick Benton. Simple relational correctness proofs for static analyses and program transformations. In *Proceedings of the 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '04)*, number MSR-TR-2005-26, page 43. ACM, January 2004.
- [5] Daniel Brown and Riccardo Pucella. Categories of timed stochastic relations. *Electronic Notes in Theoretical Computer Science*, 249:193 – 217, 2009. Proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics (MFPS 2009).
- [6] E.P de Vink and J.J.M.M Rutten. Bisimulation for probabilistic transition systems: a coalgebraic approach. *Theoretical Computer Science*, 221(1 - 2):271 – 293, 1999.
- [7] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, volume 3876 of *Lecture Notes in Computer Science*, pages 265–284. Springer Berlin Heidelberg, 2006.
- [8] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3-4):211–407, 2013.
- [9] Michèle Giry. A categorical approach to probability theory. In B. Banaschewski, editor, *Categorical Aspects of Topology and Analysis*, volume 915 of *Lecture Notes in Mathematics*, pages 68–85. Springer Berlin Heidelberg, 1982.
- [10] Bart Jacobs and Jesse Hughes. Simulations in coalgebra. *Electronic Notes in Theoretical Computer Science*, 82(1):128–149, 2003. CMCS'03, Coalgebraic Methods in Computer Science (Satellite Event for ETAPS 2003).
- [11] Shin-ya Katsumata. Parametric effect monads and semantics of effect systems. In *Proceedings of the 41st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '14, pages 633–645, New York, NY, USA, 2014. ACM.
- [12] Shin-ya Katsumata and Tetsuya Sato. Codensity Liftings of Monads. In Lawrence S. Moss and Pawel Sobocinski, editors, *6th Conference on Algebra and Coalgebra in Computer Science (CALCO 2015)*, volume 35 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 156–170, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
- [13] Kim Guldstrand Larsen and Arne Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, 1991.
- [14] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 94–103, Washington, DC, USA, 2007. IEEE Computer Society.
- [15] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *Proceedings of the Thirty-ninth Annual ACM Symposium on Theory of Computing*, STOC '07, pages 75–84, New York, NY, USA, 2007. ACM.
- [16] Federico Olmedo. *Approximate Relational Reasoning for Probabilistic Programs*. PhD thesis, Technical University of Madrid, 2014.
- [17] Prakash Panangaden. The category of markov kernels. *Electronic Notes in Theoretical Computer Science*, 22:171 – 187, 1999. PROBMIV'98, First International Workshop on Probabilistic Methods in Verification.

This appendix will be deleted from the final version of this paper.

A Appendix

We show some omitted proofs in this paper.

A.1 Proofs in Section 1.2

Proposition A.1 *The composition of the category $\mathbf{SRel} = \mathbf{Meas}_{\mathcal{G}}$ is continuous with respect to the ordering \sqsubseteq .*

Proof. Consider a measurable function $h: Y \rightarrow \mathcal{G}Z$ and an ω -chain $\{f_n: X \rightarrow \mathcal{G}Y\}_n$ with respect to \sqsubseteq . We fix $x \in X$. Since the ω -chain of measures $f_n(x)$ are bounded, and hence it converges strongly $(\sup_n f_n)(x)$. This implies that, from the definition of Lebesgue integral, for any $C \in \Sigma_Z$ and $x \in X$, we obtain

$$\begin{aligned} (h^\sharp \circ \sup_n f_n)(x)(C) &= (h^\sharp(\sup_n f_n)(x))(C) \\ &= \int_Y h(-)(C) \, d((\sup_n f_n)(x)) \\ &= \sup_n \int_Y h(-)(C) \, d(f_n(x)) \\ &= \sup_n (h^\sharp \circ f_n)(x)(C). \end{aligned}$$

Consider a measurable function $h': X \rightarrow \mathcal{G}Y$ and an ω -chain $\{f_n: Y \rightarrow \mathcal{G}Z\}_n$ with respect to \sqsubseteq . From the monotone convergence theorem, for any $C \in \Sigma_Z$ and $x \in X$, we have

$$\begin{aligned} (\sup_n f_n)^\sharp \circ h'(x)(C) &= (h^\sharp(\sup_n f_n)(x))(C) \\ &= \int_Y \sup_n f_n(-)(C) \, d(h'(x)) \\ &= \sup_n \int_Y f_n(-)(C) \, d(h'(x)) \\ &= \sup_n (f_n^\sharp \circ h')(x)(C). \end{aligned}$$

□

Lemma A.2 *If $f_1, f_2: X \rightarrow \mathcal{G}Y$ satisfy $f_1 \sqsubseteq f_2$ then $f_1 - f_2$ defined by*

$$(f_1 - f_2)(x)(B) = f_1(x)(B) - f_2(x)(B) \quad (\text{for all } x \in X, B \in \Sigma_Y)$$

is a measurable function $X \rightarrow \mathcal{G}Y$.

Proof. For each $x \in X$, the finiteness of the measures $f_1(x)$ and $f_2(x)$ imply the

countable additivity of $(f_1 - f_2)(x)$ as follows:

$$\begin{aligned}
 (f_1 - f_2)(x)(\sum_n B_n) &= f_1(x)(\sum_n B_n) - f_2(x)(\sum_n B_n) \\
 &= \sum_n f_1(x)(B_n) - \sum_n f_2(x)(B_n) \\
 &= \sum_n (f_1(x)(B_n) - f_2(x)(B_n)) \\
 &= \sum_n (f_1 - f_2)(x)(B_n)
 \end{aligned}$$

where $\sum_n B_n$ is the union of a countable disjoint collection B_0, B_1, \dots . Therefore $f_1 - f_2$ is at least a function of the form $X \rightarrow \mathcal{G}Y$.

The σ -algebra of $\mathcal{G}Y$ is generated by the following countable collection:

$$\{ \nu \in \mathcal{G}Y \mid \nu(A) \leq \alpha \} \quad (A \in \Sigma_Y, \alpha \in [0, 1] \cap \mathbb{Q}).$$

Since $f_1, f_2: X \rightarrow \mathcal{G}Y$, $A_i^\alpha = f_i^{-1}(\{ \nu \in \mathcal{G}Y \mid \nu(A) \leq \alpha \})$ is measurable for all $A \in \Sigma_Y$ and $\alpha \in [0, 1] \cap \mathbb{Q}$ ($i = 1, 2$). We then calculate

$$\begin{aligned}
 &(f_1 - f_2)^{-1}(\{ \nu \in \mathcal{G}Y \mid \nu(A) \leq \alpha \}) \\
 &= \{ x \in X \mid (f_1 - f_2)(x)(A) \leq \alpha \} \\
 &= \{ x \in X \mid f_1(x)(A) - f_2(x)(A) \leq \alpha \} \\
 &= \{ x \in X \mid f_1(x)(A) - \alpha \leq f_2(x)(A) \} \\
 &= \bigcap_{\beta \in [0, 1] \cap \mathbb{Q}} \{ x \in X \mid f_2(x)(A) \leq \beta \implies f_1(x)(A) - \alpha \leq \beta \} \\
 &= \bigcap_{\beta \in [0, 1] \cap \mathbb{Q}} \{ x \in X \mid f_2(x)(A) \leq \beta \implies f_1(x)(A) \leq \min(1, \alpha + \beta) \} \\
 &= \bigcap_{\beta \in [0, 1] \cap \mathbb{Q}} ((X \setminus A_2^\beta) \cup A_1^{\min(1, \alpha + \beta)})
 \end{aligned}$$

Hence, the function $f_1 - f_2$ is measurable. \square

A.2 Proofs in Section 2.2

We recall the definition of the *indicator function* $\chi_A: X \rightarrow [0, 1]$ of a subset $A \subseteq X$:

$$\chi_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

The subset A of X is a measurable *if and only if* the indicator function χ_A is a measurable function $: X \rightarrow [0, 1]$.

Lemma A.3 *The following equation holds for any (Φ, X, Y) in $\mathbf{BRel}(\mathbf{Meas})$:*

$$\mathcal{G}^{(\gamma, \delta)} \Phi = \left\{ (\nu_1, \nu_2) \mid \forall (f, g): \Phi \rightarrow \leq \text{ in } \mathbf{BRel}(\mathbf{Meas}). \int_X f \, d\nu_1 \leq \gamma \int_Y g \, d\nu_2 + \delta \right\},$$

Proof. We recall

$$\mathcal{G}^{(\gamma, \delta)}\Phi = \left\{ (\nu_1, \nu_2) \in \mathcal{GX} \times \mathcal{GY} \left| \begin{array}{l} \forall A \in \Sigma_X, B \in \Sigma_Y. \\ \Phi(A) \subseteq B \implies \nu_1(A) \leq \gamma \nu_2(B) + \delta \end{array} \right. \right\}.$$

(\supseteq) Suppose the pair (ν_1, ν_2) satisfies $\int_X f d\nu_1 \leq \gamma \int_Y g d\nu_2 + \delta$ for all $(f, g): \Phi \rightarrow \leq$ in $\mathbf{BRel}(\mathbf{Meas})$.

Assume that $A \in \Sigma_X$ and $B \in \Sigma_Y$ satisfy $\Phi(A) \subseteq B$. The indicator functions $\chi_A: X \rightarrow [0, 1]$, $\chi_B: Y \rightarrow [0, 1]$ are measurable, and satisfy $\chi_A(x) \leq \chi_B(y)$ for any $(x, y) \in \Phi$ because $(x, y) \in \Phi \wedge x \in A \implies y \in \Phi(A)$. These imply that (χ_A, χ_B) is an arrow $\Phi \rightarrow \leq$ in $\mathbf{BRel}(\mathbf{Meas})$. We then obtain $\int_X \chi_A d\nu_1 \leq \gamma \int_Y \chi_B d\nu_2 + \delta$, which is equivalent to $\nu_1(A) \leq \gamma \nu_2(B) + \delta$.

(\subseteq) Suppose $(\nu_1, \nu_2) \in \mathcal{G}^{(\gamma, \delta)}\Phi$. Take an arbitrary arrow $(f, g): \Phi \rightarrow \leq$ in $\mathbf{BRel}(\mathbf{Meas})$. We have $f^{-1}([\beta, 1]) \in \Sigma_X$ and $g^{-1}([\beta, 1]) \in \Sigma_Y$. We obtain $\Phi(f^{-1}([\beta, 1])) \subseteq g^{-1}([\beta, 1])$ for any $\beta \in [0, 1]$ because $(x, y) \in \Phi \wedge f(x) \geq \beta \implies g(y) \geq \beta$. By the definition of Lebesgue integration, we calculate as follows:

$$\begin{aligned} & \int_X f d\nu_1 \\ &= \sup \left\{ \sum_{k=0}^n \alpha_k \nu_1(f^{-1}([\sum_{l=0}^k \alpha_l, 1])) \left| n \in \mathbb{N}, \{\alpha_k\}_{k=1}^n \text{ s.t. } \sum_{k=0}^n \alpha_k \leq 1, \forall k. (0 \leq \alpha_k) \right. \right\} \\ &\leq \sup \left\{ \sum_{k=0}^n \alpha_k (\gamma \nu_2(g^{-1}([\sum_{l=0}^k \alpha_l, 1])) + \delta) \left| n \in \mathbb{N}, \{\alpha_k\}_{k=1}^n \text{ s.t. } \sum_{k=0}^n \alpha_k \leq 1, \forall k. (0 \leq \alpha_k) \right. \right\} \\ &\leq \gamma \sup \left\{ \sum_{k=0}^n \alpha_k \nu_2(g^{-1}([\sum_{l=0}^k \alpha_l, 1])) \left| n \in \mathbb{N}, \{\alpha_k\}_{k=1}^n \text{ s.t. } \sum_{k=0}^n \alpha_k \leq 1, \forall k. (0 \leq \alpha_k) \right. \right\} + \delta \\ &= \gamma \int_Y g d\nu_2 + \delta. \end{aligned}$$

Here, the first and last equality are given by definition of Lebesgue integration. The first inequality is obtained from the assumption $(\nu_1, \nu_2) \in \mathcal{G}^{(\gamma, \delta)}\Phi$. The second inequality is obtained from the condition $\sum_{k=0}^n \alpha_k \leq 1$. \square

A.3 Proofs in Section 3.4

Lemma A.4 *The rule [rand] is sound.*

Proof. We assume $x_1 \neq x_2$ since the soundness is obvious when $x_1 = x_2$. We then obtain $\Gamma = \Gamma, x_1: \tau, x_2: \tau$ from the precondition of the rule [rand]. Hence, we may assume $\llbracket \Gamma \rrbracket = \llbracket \Gamma' \rrbracket \times \llbracket \tau \rrbracket \times \llbracket \tau \rrbracket$. It suffices to show

$$\begin{aligned} & (m_1, m_2) \in \Psi \\ & \implies ((\llbracket \Gamma \vdash x_1 \stackrel{\$}{\leftarrow} d(e_1^1, \dots, e_m^1) \rrbracket(m_1), \llbracket \Gamma \vdash x_2 \stackrel{\$}{\leftarrow} d(e_1^2, \dots, e_m^2) \rrbracket(m_2)) \in \mathcal{G}^{(\gamma, \delta)}(\Phi), \end{aligned}$$

where

$$\Phi = (x_1 \langle 1 \rangle = x_2 \langle 2 \rangle) = \{ (m_1, m_2) \mid \pi_{x_1}(m_1) = \pi_{x_2}(m_2) \}.$$

Let $(m_1, m_2) \in \Psi$ and $A \in \Sigma_{[\Gamma]}$. We have $\Phi(A) = [\Gamma'] \times [\tau] \times A_{x_1}$, where $A_{x_1} = \{\pi_3(m) \mid m \in A\}$. We remark that A_{x_1} is measurable, and therefore so is $\Phi(A)$.

We denote by ν_i the measure $\llbracket d \rrbracket(\llbracket \Gamma \vdash^t e_i^i \rrbracket(m_i), \dots, \llbracket \Gamma \vdash^t e_m^i \rrbracket(m_i))$ ($i = 1, 2$).

$$\begin{aligned}
 \llbracket \Gamma \vdash x_1 \stackrel{\$}{\leftarrow} d(e_1^1, \dots, e_m^1) \rrbracket(m_1)(A) &= \mathcal{G}(\rho_{(x_1: \tau, \Gamma)}) \circ \text{st}_{[\tau], [\Gamma]} \circ \langle \nu_1, m_1 \rangle(A) \\
 &= \text{st}_{[\tau], [\Gamma]}^{\mathcal{G}}(\nu_1, m_1)(\rho_{(x_1: \tau, \Gamma)}^{-1}(A)) \\
 &= (\nu_1 \otimes \delta_{m_1})(\rho_{(x_1: \tau, \Gamma)}^{-1}(A)) \\
 &= \int_{[\tau] \times [\Gamma]} \chi_{\rho_{(x_1: \tau, \Gamma)}^{-1}(A)} d(\nu_1 \otimes \delta_{m_1}) \\
 &= \int_{a \in [\tau]} \left(\int_{[\Gamma]} \chi_{\rho_{(x_1: \tau, \Gamma)}^{-1}(A)}(a, -) d(\delta_{m_1}) \right) d\nu_1 \\
 &= \int_{[\tau]} f d\nu_1 \\
 \llbracket \Gamma \vdash x_2 \stackrel{\$}{\leftarrow} d(e_1^2, \dots, e_m^2) \rrbracket(m_2)(\Phi(A)) &= \llbracket \Gamma \vdash x_2 \stackrel{\$}{\leftarrow} d(e_1^2, \dots, e_m^2) \rrbracket(m_2)([\Gamma'] \times [\tau] \times A_{x_1}) \\
 &= (\nu_2 \otimes \delta_{m_2})(\rho_{(x_2: \tau, \Gamma)}^{-1}([\Gamma'] \times [\tau] \times A_{x_1})) \\
 &= (\nu_2 \otimes \delta_{m_2})(A_{x_1}) \\
 &= \int_{[\tau]} g d\nu_2,
 \end{aligned}$$

Where, $f = \chi_{(\rho_{(x_1: \tau, \Gamma)}^{-1}(-, m_1))^{-1}(A)}$ and $g = \chi_{A_{x_1}}$. The pair of these arrows (f, g) forms an arrow $\text{Eq}_{[\tau]} \rightarrow \leq$ in **BRel(Meas)**. Hence we obtain from Lemma A.3,

$$\llbracket \Gamma \vdash x_1 \stackrel{\$}{\leftarrow} d(e_1^1, \dots, e_m^1) \rrbracket(m_1)(A) \leq \gamma \llbracket \Gamma \vdash x_2 \stackrel{\$}{\leftarrow} d(e_1^2, \dots, e_m^2) \rrbracket(m_2)(A) + \delta.$$

Since A is arbitrary, we conclude

$$(\llbracket \Gamma \vdash x_1 \stackrel{\$}{\leftarrow} d(e_1^1, \dots, e_m^1) \rrbracket(m_1), \llbracket \Gamma \vdash x_2 \stackrel{\$}{\leftarrow} d(e_1^2, \dots, e_m^2) \rrbracket(m_2)) \in \mathcal{G}^{(\gamma, \delta)}(\Phi)$$

□

Lemma A.5 *The rule [cond] is sound.*

Proof. Let $(m_1, m_2) \in \Psi$. We have $\llbracket \Gamma \vdash b \rrbracket(m_1) = \llbracket \Gamma \vdash b' \rrbracket(m_2)$ from the preconditions of the rule [cond]. Since

$$\llbracket \Gamma \vdash \text{if } b \text{ then } c_1 \text{ else } c_2 \rrbracket = [\llbracket \Gamma \vdash c_1 \rrbracket, \llbracket \Gamma \vdash c_2 \rrbracket] \circ \cong_{[\Gamma]} \circ \langle \llbracket \Gamma \vdash b \rrbracket, \text{id}_{[\Gamma]} \rangle,$$

we have the following two cases:

(i) When $\llbracket \Gamma \vdash b \rrbracket(m_1) = \iota_1(*)$, we obtain

$$\begin{aligned}
 \llbracket \Gamma \vdash \text{if } b \text{ then } c_1 \text{ else } c_2 \rrbracket(m_1) &= \llbracket \Gamma \vdash c_1 \rrbracket(m_1) \\
 \llbracket \Gamma \vdash \text{if } b' \text{ then } c'_1 \text{ else } c'_2 \rrbracket(m_2) &= \llbracket \Gamma \vdash c'_1 \rrbracket(m_2)
 \end{aligned}$$

We then obtain

$$(\llbracket \Gamma \vdash \text{if } b \text{ then } c_1 \text{ else } c_2 \rrbracket(m_1), \llbracket \Gamma \vdash \text{if } b' \text{ then } c'_1 \text{ else } c'_2 \rrbracket(m_2)) \in \overline{\mathcal{G}^{(\gamma, \delta)}}\Phi. \quad (\text{A.1})$$

(ii) When $\llbracket \Gamma \vdash b \rrbracket(m_1) = \iota_2(*)$, we obtain (A.1) similarly. \square

Lemma A.6 *The rule [while] is sound.*

Proof. We first prove by induction on n :

$$\begin{aligned} \models [\text{while } b_1 \text{ do } c_1]_n &\sim_{(\prod_{k=0}^{n-1}, \gamma_k \sum_{k=0}^{n-1} \delta_k)} [\text{while } b_2 \text{ do } c_2]_n : \\ \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq k &\Rightarrow \Theta \wedge e \langle 1 \rangle \geq n + k \end{aligned} \quad (\text{A.2})$$

case: $n = 0$ We obtain $\models \text{null} \sim_{(1,0)} \text{null} : \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq k \Rightarrow \emptyset$ since $\llbracket \Gamma \vdash \text{null} \rrbracket$ is the null measure over $\llbracket \Gamma \rrbracket$. We recall that the following equality:

$$[\text{while } b_i \text{ do } c_i]_0 = \text{if } b_i \text{ then null else skip},$$

We obtain from the above equality, (A.2) by applying [skip], [cond], and [weak].

case: $n = m + 1$ From the precondition of [while] and the soundness of [case],

$$\models c_1 \sim_{(\gamma_m, \delta_m)} c_2 : \Theta \wedge (e \langle 1 \rangle = k) \implies (e \langle 1 \rangle > k)$$

By the induction hypothesis,

$$\begin{aligned} \models [\text{while } b_1 \text{ do } c_1]_m &\sim_{(\prod_{k=0}^{m-1}, \gamma_k \sum_{k=0}^{m-1} \delta_k)} [\text{while } b_2 \text{ do } c_2]_m : \\ \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq k &\Rightarrow \Theta \wedge e \langle 1 \rangle \geq m + k \end{aligned}$$

From the soundness of the rule [seq], we obtain

$$\begin{aligned} \models c_1; [\text{while } b_1 \text{ do } c_1]_m &\sim_{(\prod_{k=0}^m, \gamma_k \sum_{k=0}^m \delta_k)} c_2; [\text{while } b_2 \text{ do } c_2]_m : \\ \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq k &\Rightarrow \Theta \wedge e \langle 1 \rangle \geq m + 1 + k \end{aligned}$$

From the soundness of [weak], [cond], and [skip] we conclude (A.2).

It is obvious that $\Theta \Rightarrow b_1 \langle 1 \rangle = b_2 \langle 2 \rangle$ implies

$$\models \text{while } b_1 \text{ do } c_1 \sim_{(1,0)} \text{while } b_2 \text{ do } c_2 : \Theta \wedge \neg \wedge b_1 \langle 1 \rangle \Rightarrow \Theta \wedge \neg b_1 \langle 1 \rangle. \quad (\text{A.3})$$

From (A.2) and (A.3), and the soundness of [cond] and [seq], we obtain

$$\begin{aligned} \models [\text{while } b_1 \text{ do } c_1]_n; \text{while } b_1 \text{ do } c_1 &\sim_{(\prod_{k=0}^m \gamma_k, \sum_{k=0}^m \delta_k)} [\text{while } b_2 \text{ do } c_2]_n; \text{while } b_2 \text{ do } c_2 : \\ \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq 0 &\Rightarrow \Theta \wedge \neg b_1 \langle 1 \rangle \end{aligned}$$

Since $\mathbf{SRel} = \mathbf{Meas}_{\mathcal{G}}$ is $\omega\mathbf{CPO}_{\perp}$ -enriched, for any command c and expression of the type `bool`, we obtain $\llbracket \Gamma \vdash [\text{while } b \text{ do } c]_n; \text{while } b \text{ do } c \rrbracket = \llbracket \Gamma \vdash \text{while } b \text{ do } c \rrbracket$. Hence,

$$\begin{aligned} \models \text{while } b_1 \text{ do } c_1 &\sim_{(\prod_{k=0}^m \gamma_k, \sum_{k=0}^m \delta_k)} \text{while } b_2 \text{ do } c_2 : \\ \Theta \wedge b_1 \langle 1 \rangle \wedge e \langle 1 \rangle \geq 0 &\Rightarrow \Theta \wedge \neg b_1 \langle 1 \rangle \end{aligned}$$

□

Lemma A.7 *The rule [frame] is sound.*

Proof. Let $(m_1, m_2) \in \Psi \wedge \Theta$, $\nu_1 = \llbracket \Gamma \vdash c_1 \rrbracket(m_1)$, and $\nu_2 = \llbracket \Gamma \vdash c_2 \rrbracket(m_2)$. Since $(\nu_1, \nu_2) \in \text{Range}(\Theta)$, there exist $A', B' \in \Sigma_{\llbracket \Gamma \rrbracket}$ such that $A' \times B' \subseteq \Theta$, and $\nu_1(C) = \nu_1(C \wedge A')$ and $\nu_2(D) = \nu_2(D \wedge B')$ for all $C, D \in \Sigma_{\llbracket \Gamma \rrbracket}$. Suppose that $A, B \in \Sigma_{\llbracket \Gamma \rrbracket}$ satisfy $(\Phi \wedge \Theta)(A) \subseteq B$. Since $A' \times B' \subseteq \Theta$, we have $(\Phi \wedge (A' \times B'))(A) \subseteq B$. This implies $\Phi(A \wedge A') \wedge B' \subseteq B$. Thus, $\Phi(A \wedge A') \subseteq B + (\llbracket \Gamma \rrbracket \setminus (B \vee B'))$. Therefore

$$\begin{aligned} \nu_1(A) &= \nu_1(A \wedge A') \leq \gamma \nu_2(B + (M \setminus (B \vee B'))) + \delta \\ &= \gamma \nu_2((B + (M \setminus (B \vee B'))) \wedge B') + \delta \leq \gamma \nu_2(B \wedge B') + \delta \leq \gamma \nu_2(B) + \delta. \end{aligned}$$

Hence, $(\nu_1, \nu_2) \in \mathcal{G}(\Theta \wedge \Phi)$. Similarly, we obtain $(\nu_1, \nu_2) \in (\mathcal{G}(\Theta \wedge \Phi))^\Phi$. □

A.4 Proofs in Section 3.5

Proposition A.8 (Proposition 3.2) *Let $f: X \times Y \rightarrow \mathbb{R}$ be a positive measurable function, and ν be a measure over Y . For all $a, a' \in X$, $\gamma, \gamma' \geq 1$, $\delta \geq 0$, and $Z \in \Sigma_Y$ (window set), if the following three conditions hold then for any $B \in \Sigma_Y$, we have $f_a(B) \leq \gamma \gamma' f_{a'}(B) + \delta$.*

- (i) $0 < \frac{1}{\gamma'} \int_Y f(a', -) d\nu \leq \int_Y f(a, -) d\nu < \infty$
- (ii) $\forall b \in Z. f(a, b) \leq \gamma f(a', b)$
- (iii) $f_a(Y \setminus Z) \leq \delta$,

Proof. From the conditions of this proposition, we obtain for each $B \in \Sigma_Y$,

$$\begin{aligned} f_a(B) &= f_a(B \cap Z) + f_a(B \setminus Z) \\ &\leq \frac{\gamma \int_{B \cap Z} f(a', -) d\nu}{\int_Y f(a, -) d\nu} + \delta \\ &\leq \frac{\gamma \int_{B \cap Z} f(a', -) d\nu}{\frac{1}{\gamma'} \int_Y f(a', -) d\nu} + \delta \\ &\leq \gamma \gamma' f_{a'}(B) + \delta. \end{aligned}$$

Lemma A.9 (Laplacian Mechanism) *If $|a - a'| < r$ then the following parameters satisfy the conditions (i)–(iii): $\gamma = \exp(r/\sigma)$, $\gamma' = 1$, $\delta = 0$, the function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(a, b) = \frac{2}{\sigma} \exp(\frac{-|b-a|}{\sigma})$, the Lebesgue measure ν over \mathbb{R} , and the window $Z = \mathbb{R}$.* □

Proof. The conditions (i) is satisfied, because the function $f(a, -)$ is the density function of Laplacian distribution, and hence $\int_{\mathbb{R}} f(a, -) d\nu = \int_{\mathbb{R}} f(a', -) d\nu = 1$.

The condition (iii) is automatically satisfied since $\mathbb{R} \setminus Z = \emptyset$.

We now check that the condition (ii) is satisfied. The triangle inequality $|b - a'| \leq |a - a'| + |b - a|$ and the assumption $|a - a'| < r$ imply:

$$\frac{f(a, b)}{f(a', b)} = \exp\left(\frac{|b - a'| - |b - a|}{\sigma}\right) \leq \exp\left(\frac{|a - a'|}{\sigma}\right) \leq \exp\left(\frac{r}{\sigma}\right)$$

This implies $f(a, b) \leq \exp(r/\sigma)f(a', b)$. \square

Lemma A.10 (Exponential Mechanism) *Let D be the discrete Euclidian space \mathbb{Z}^n , and (R, ν) be a (positive) measure space. Let $q: D \times R \rightarrow \mathbb{R}$ be a measurable function such that $\sup_{b \in R} |q(a, b) - q(a', b)| \leq c \cdot \|a - a'\|_1$ for some $c > 0$. Suppose $0 < \int_R \exp(\varepsilon q(a, -)) d\nu < \infty$ for any $a \in D$.*

Suppose $\|a - a'\|_1 < r$. The following parameters then satisfy the conditions (i)–(iii): $\gamma = \gamma' = \exp(\varepsilon r c)$, $\delta = 0$, the function $f: D \times R \rightarrow \mathbb{R}$ defined by $f(a, b) = \exp(\varepsilon q(a, b))$ with fixed $\varepsilon > 0$, the given measure ν , and the window $Z = R$.

Proof. The condition (iii) is obviously satisfied.

The conditions (i) and (ii) is obtained from the following calculation: whenever $\|a - a'\|_1 < r$, we obtain

$$\begin{aligned} \frac{f(a, b)}{f(a', b)} &= \exp(\varepsilon q(a, b) - \varepsilon q(a', b)) \leq \exp(\varepsilon |q(a, b) - q(a', b)|) \\ &\leq \exp(\varepsilon c \|a - a'\|_1) \leq \exp(\varepsilon c r) \end{aligned}$$

\square

Lemma A.11 (Gaussian Mechanism: Relaxed Result of [8, Theorem A.1])

If $|a - a'| < r$, $1 < \gamma < \exp(1)$, and $\gamma' = 1$ hold, and $c = \frac{\sigma \log \gamma}{r}$ satisfies $((1 + \sqrt{3})/2) < c$ and $2 \log(0.66/\delta) < c^2$, then the parameters γ , γ' , and δ , the function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(a, b) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{(b-a)^2}{2\sigma^2})$, and the Lebesgue measure ν over \mathbb{R} satisfy the conditions (i)–(iii) of Proposition 3.2 for the window set Z given by

$$Z = \begin{cases} \{ b \mid b \leq (a + a')/2 + (\sigma^2 \log \gamma / r) \}, & \text{if } a \leq a' \\ \{ b \mid b \geq (a + a')/2 - (\sigma^2 \log \gamma / r) \}, & \text{if } a' \leq a. \end{cases}$$

Proof. We assume $a' \leq a$ because in the case $a' > a$, we can prove in the similar way as $a' \leq a$.

The conditions (i) is satisfied, because for each $a \in \mathbb{R}$ the function $f(a, -)$ is the density function of Gaussian distribution, and hence $\int_{\mathbb{R}} f(a, -) d\nu = \int_{\mathbb{R}} f(a', -) d\nu = 1$.

We prove that the given parameters satisfy the condition (ii) of Proposition 3.2. Suppose $Z = \{ b \mid b \leq (a + a')/2 + (\sigma^2 \log \gamma / r) \}$. Take an arbitrary $b \in Z$. We then calculate as follows:

$$\begin{aligned} \frac{f(a, b)}{f(a', b)} &= \exp\left(\frac{(b - a')^2 - (b - a)^2}{2\sigma^2}\right) \\ &= \exp\left(\frac{1}{\sigma^2}(a - a')(b - \frac{a + a'}{2})\right) \\ &\leq \exp\left(\frac{r}{\sigma^2}(b - \frac{a + a'}{2})\right) \\ &\leq \exp\left(\frac{r}{\sigma^2} \frac{\sigma^2 \log \gamma}{r}\right) \leq \gamma \end{aligned}$$

This implies $\forall b \in Z. f(a, b) \leq \gamma f(a', b)$.

We prove that given parameters satisfy the condition (iii). Let $H = \frac{a+a'}{2} + \frac{\sigma^2 \log \gamma}{r}$, and let $H' = \frac{a'-a}{2\sigma} + \frac{\sigma \log \gamma}{r}$.

Since $c > ((1 + \sqrt{3})/2)$, we have $c - \frac{1}{2c} - 1 > 0$. From $\log \gamma < 1$, we obtain $c - \frac{\log \gamma}{2c} - 1 > 0$. Since $-r < a' - a$, we obtain $H' > 1$, and hence $\log(H') > 0$.

Since $c^2 > 2 \log(0.66/\delta)$, we have $c^2 > 2 \log(\frac{1}{\delta} \sqrt{\frac{\exp(1)}{2\pi}})$. This implies $c^2 - 1 > 2 \log(\frac{1}{\delta \sqrt{2\pi}})$. Since $H' > c - \frac{\log \gamma}{2c} > c - \frac{1}{2c}$, we then obtain $H'^2 > c^2 - 1 > 2 \log(\frac{1}{\delta \sqrt{2\pi}})$. Therefore, we conclude $\log(H') + H'^2/2 > \log(\frac{1}{\delta \sqrt{2\pi}})$.

We then obtain:

$$\begin{aligned} & \int_{\mathbb{R} \setminus Z} \frac{1}{\sigma \sqrt{2\pi}} \exp\left(-\frac{(x-a)^2}{2\sigma^2}\right) d\nu \\ &= \frac{1}{\sigma \sqrt{2\pi}} \int_H^\infty \exp\left(-\frac{(x-a)^2}{2\sigma^2}\right) dx \\ &= \frac{1}{\sqrt{2\pi}} \int_{H'}^\infty \exp\left(-\frac{b^2}{2}\right) db \\ &\leq \frac{1}{\sqrt{2\pi}} \int_{H'}^\infty \frac{b}{H'} \exp\left(-\frac{b^2}{2}\right) db \\ &\leq \frac{1}{\sqrt{2\pi} H'} \exp\left(-\frac{H'^2}{2}\right) \leq \delta. \end{aligned}$$

This implies $f_a(\mathbb{R} \setminus Z) \leq \delta$. □

A.5 Proofs in Section 4

Lemma A.12 (Lemma 4.1) *If $x: \tau$ and the space $\llbracket \tau \rrbracket$ is countable discrete then*

$$\bigcap_{i \in \llbracket \tau \rrbracket} \mathcal{G}^{(\gamma, \delta_i)}(x\langle 1 \rangle = i \Rightarrow x\langle 2 \rangle = i) \subseteq \mathcal{G}^{(\gamma, \sum_{i \in \llbracket \tau \rrbracket} \delta_i)}(x\langle 1 \rangle = x\langle 2 \rangle).$$

Proof. Let $\llbracket \Gamma, x: \tau \rrbracket = \llbracket \tau \rrbracket \times \llbracket \Gamma \rrbracket$. Suppose $(\nu_1, \nu_2) \in \bigcap_{i \in \llbracket \tau \rrbracket} \mathcal{G}^{(\gamma, \delta_i)}(x\langle 1 \rangle = i \Rightarrow x\langle 2 \rangle = i)$. Take an arbitrary $A \in \Sigma_{\llbracket \Gamma, x: \tau \rrbracket}$. Since $\llbracket \tau \rrbracket$ is countable discrete, we decompose $A = \sum_{i \in \llbracket \tau \rrbracket} (\{i\} \times A_i)$. We may assume $A_i \neq \emptyset$ because $\{i\} \times \emptyset = \emptyset$. Since $(x\langle 1 \rangle = i \Rightarrow x\langle 2 \rangle = i)(\{i\} \times A_i) = \{i\} \times \llbracket \Gamma \rrbracket$, we obtain $\nu_1(\{i\} \times A_i) \leq \gamma \nu_2(\{i\} \times \llbracket \Gamma \rrbracket) + \delta_i$ for each $i \in \llbracket \tau \rrbracket$. By summing them up, we obtain $\nu_1(A) \leq \gamma \nu_2((x\langle 1 \rangle = x\langle 2 \rangle)(A)) + \sum_{i \in \llbracket \tau \rrbracket} \delta_i$. □